IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BRITISH TELECOMMUNICATIONS PLC and BT AMERICAS, INC., Plaintiff, v. FORTINET, INC., Defendant.	Civil Action No. 18-1018-CFC

MEMORANDUM ORDER

Plaintiffs British Telecommunications PLC and BT Americas, Inc. (collectively BT), have sued Defendant Fortinet, Inc., for infringement of U.S. Patent Nos. 7,159,237 (the #237 patent), 7,370,358 (the #358 patent), 7,693,971 (the #971 patent), 7,774,845 (the #845 patent), and 7,895,641 (the #641 patent). D.I. 1. The Magistrate Judge held a *Markman* hearing for the asserted patents on November 18, 2020 and issued a Report and Recommendation on April 15, 2021. D.I. 141. Both BT and Fortinet filed objections, collectively disputing seven claim constructions. D.I. 142; D.I. 143.

I review de novo the Magistrate Judge's conclusions. *See St. Clair Intellectual Prop. Consultants, Inc. v. Matsushita Elec. Indus. Co.*, 691 F. Supp. 2d 538, 541–42 (D. Del. 2010) ("Objections to the magistrate judge's conclusions

with regard to the legal issue of claim construction are reviewed *de novo*."); Fed. R. Civ. P. 72(b)(3).

I. BACKGROUND

The asserted patents cover systems and methods for monitoring computer networks to detect security threats. The #237 and #641 patents share a common written description. Claim 1 of the #237 patent recites

> [a] method of operating a probe as part of a security monitoring system for a computer network, comprising:
> a) collecting status data from at least one monitored component of said network;
> b) analyzing status data to identify potentially security related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
> c) transmitting information about said identified events to an analyst associated with said security monitoring system;
> d) receiving feedback at the probe based on empirically derived information reflecting operation of said security monitoring system; and
> e) dynamically modifying an analysis capability of said probe during operation thereof based on said received feedback.

Claim 1 of the #358 patent recites

> [a] computer security system comprising:
> a plurality of inter-communicating computers including software agents together forming a plurality of agent groups, each agent corresponding with other agents in its

> respective group but not with agents in other groups via a message-exchange system including the exchange of group specific tags;
> means for maintaining and tracking groupwide measures of agent status or behavior, and
> means for comparing actual behavior patterns of the measure for a given group with known normal behavior patterns and determining that a security threat does or may exist when the actual behavior patterns diverge from normal behavior patterns.

Claim 1 of the #971 patent recites

> [a] computer network management system comprising:
> a communication network having a policy-based manager means distributed across said network,
> the distributed policy-based manager comprising a plurality of distributed management agents arranged in a hierarchy and being associated with sub-networks of said network, each of said agents includes means to register local network components with itself, to identify and store one or more roles associated with the component and to obtain policies relevant to the stored roles of the registered components,
> wherein each of the policies are locally stored and specify a subject role identifying the components in the system which are expected to respond to a policy and an action element specifying an action to be carried out.

Claim 1 of the #845 patent recites

> [a] computer security system for use in a network environment comprising at least a group of user computers arranged to communicate over a network, the system comprising:

a warning message exchange system operable to allow communications from the group of user computers of warning messages relating to a piece or set of suspect data identified by one or more of the group of user computers as a possible security threat;
an identity generator operable to generate an identifier of the piece or set of suspect data;
a message counting system operable to maintain a count for every particular piece or set of suspect data based on a number of warning messages communicated over the network relating to each of the piece or set of suspect data;
and a network security system operable to act in respect of any particular piece or set of suspect data when the count maintained therefor is substantially equal to or greater than at least one threshold value, wherein the threshold value is greater than one.

Claim 1 of the #641 patent recites

[a] system for operating a probe as part of a security monitoring system for a computer network, the system comprising:
a) a sensor coupled to collect status data from at least one monitored component of the network;
b) a filtering subsystem coupled to analyze status data to identify potentially security-related events represented in the status data, wherein the analysis includes filtering followed by an analysis of post-filtering residue, wherein the post-filtering residue is data neither discarded nor selected by filtering;
c) a communications system coupled to transmit information about the identified events to an analyst system associated with the security monitoring system;
d) a receiver for receiving feedback at the probe based on empirically-derived information reflecting operation of the security monitoring system; and

e) a modification control system for dynamically modifying an analysis capability of the probe during operation thereof based on the received feedback.

II. LEGAL STANDARDS FOR CLAIM CONSTRUCTION

"It is a bedrock principle of patent law that the claims of a patent define the invention to which the patentee is entitled the right to exclude." *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc). "'[T]here is no magic formula or catechism for conducting claim construction.' Instead, the court is free to attach the appropriate weight to appropriate sources 'in light of the statutes and policies that inform patent law.'" *SoftView LLC v. Apple Inc.*, 2013 WL 4758195, at *1 (D. Del. Sept. 4, 2013) (quoting *Phillips*, 415 F.3d at 1324). It is necessary to construe claim terms whenever there is a fundamental dispute between parties about their meaning. *O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Col., Ltd.*, 521 F.3d 1352, 1362 (Fed. Cir. 2008). Construing the claims of a patent is a question of law. *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 977–78 (Fed. Cir. 1995), *aff'd*, 517 U.S. 370, 388–90 (1996).

Unless a patentee acts as its own lexicographer by setting forth a special definition or disavows the full scope of a claim term, the words in a claim are to be given their ordinary and accustomed meaning. *Thorner v. Sony Comput. Ent. Am. LLC*, 669 F.3d 1362, 1365 (Fed. Cir. 2012). "[T]he ordinary and customary meaning of a claim term is the meaning that the term would have to a person of

ordinary skill in the art in question at the time of the invention, i.e., as of the effective filing date of the patent application." *Phillips*, 415 F.3d at 1313. An artisan of ordinary skill "is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent." *Id.* at 1313.

"[T]he specification is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term." *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996).[1] A patent's prosecution history, although "less useful for claim construction purposes," is intrinsic evidence and can reveal "how the inventor understood the invention and whether the inventor limited the invention in the course of prosecution." *Phillips*, 415 F.3d at 1317. A disclaimer during patent prosecution will limit the plain and ordinary meaning of claim language when the

[1] Section 112(b) of Title 35 provides that "[t]he specification shall conclude with one or more claims[.]" This language makes clear that the specification includes the claims asserted in the patent, and the Federal Circuit has so held. *See Markman*, 52 F.3d at 979 ("Claims must be read in view of the specification, of which they are part"). The Federal Circuit and other courts, however, have also used "specification" on occasion to refer to the written description of the patent as distinct from the claims. *See, e.g., id.* ("To ascertain the meaning of claims, we consider three sources: The claims, the specification, and the prosecution history."). To avoid confusion, I will refer to the portion of the specification that is not the claims or figures as "the written description."

patentee made statements that "amount to a clear and unmistakable disclaimer limiting the meaning of the claim terms." *Massachusetts Inst. of Tech. v. Shire Pharm., Inc.*, 839 F.3d 1111, 1119 (Fed. Cir. 2016); *see also Aylus Networks, Inc. v. Apple Inc.*, 856 F.3d 1353, 1360 (Fed. Cir. 2017) (holding that the scope of claims can be limited by a patentee's statements during inter partes review (IPR) proceedings).

The court may also consider extrinsic evidence, which "consists of all evidence external to the patent and prosecution history, including expert and inventor testimony, dictionaries, and learned treatises." *Id.* "Extrinsic evidence is to be used for the court's understanding of the patent, not for the purpose of varying or contradicting the terms of the claims." *Markman*, 52 F.3d at 981. "The construction that stays true to the claim language and most naturally aligns with the patent's description of the invention will be, in the end, the correct construction." *Renishaw PLC v. Marposs Societa' per Azioni*, 158 F.3d 1243, 1250 (Fed. Cir. 1998).

III. DISPUTED TERMS FROM THE #237 AND #641 PATENTS

A. "status data" (#237 patent claims 1, 2, 6, 10, 14, 16, 18, 22–27, 31, 35, 41; #641 patent claims 1, 2, 6, 10, 14, 16)

1. BT's Construction: "data extracted from or generated about the traffic or system processing it that is informative as to the status of the network and its components"

2. Fortinet's Initial Construction: "data extracted from or generated about the traffic or system processing the data that reflects the conditions of the network and its components at a given time"

3. Fortinet's Current Construction: "data extracted from or generated about traffic or systems processing it that is informative as the conditions of data, the network and its components"

4. Report and Recommendation's Construction: "data extracted from or generated about the traffic or system processing it that is informative as to the status of the network and its components"

5. The Court's Construction: "data extracted from or generated about the traffic or system processing it that is informative as to the status of the network and its components"

Fortinet faults the Report and Recommendation's construction for being "circular and ambiguous" because it "reus[es] without elucidating meaning for the term 'status.'" D.I. 143 at 1. Fortinet argues that "instead of using ['status'] tautologically," I should revise the "status of the network and its components" clause in the recommended construction to read "conditions of data, the network, and its components." D.I. 143 at 2. In other words, Fortinet asks me to delete the word "status" from the recommended construction in order to avoid reusing that word, but at the same time add (and thus reuse) the word "data" in the construction of the clause. Fortinet never presented this argument to the Magistrate Judge; but in any event, I do not believe that using "condition" in place of "status" would clarify the meaning of "status data" or assist the trier of fact. Accordingly, I will adopt the Magistrate Judge's recommendation for this term.

B. "**dynamically**" (#237 patent claims 1, 2, 6, 10, 14, 16, 18, 22–27, 31, 35, 39, 41; #641 patent claims 1, 2, 6, 10, 14, 16)

1. BT's Construction: "during actual operation, rather than offline"
2. Fortinet's Initial Construction: "during actual operation"
3. Fortinet's Current Construction: "during actual operation, rather than offline or in idle mode"
4. Report and Recommendation Construction: "during actual operation, rather than offline"
5. The Court's Construction: "during actual operation, rather than offline"

Fortinet objects to the recommended construction on the grounds that the phrase "rather than offline" ambiguously suggests that "offline" is the inverse of "actual operation." D.I. 143 at 2. Fortinet is again asking me to adopt a construction that it has not previously argued for. Neither party has offered a meaning for "idle mode," a term not used in the patents. I will not consider a new construction that was not fully briefed in the record before me. Accordingly, I will adopt the Magistrate Judge's recommendation for this term.

C. "**probe**" (#237 patent claims 1, 6, 10, 14, 18, 22–26, 31, 25, 29; #641 patent claims 1, 6, 10, 14)

1. BT's Construction: "a system that collects data from one or more network components to which it is attached, filters or otherwise analyzes the data that has been collected, transmits noteworthy information, and receives feedback in order to update its capabilities of analysis"
2. Fortinet's Construction: "a discrete software or hardware component that performs an initial scan and analysis of traffic of at least one network component to which it is attached;"

or alternatively, "a discrete component that collects data from one or more network components to which it is attached, filters or otherwise analyzes the data that had been collected, transmits noteworthy information, and receives feedback in order to update its capabilities of analysis"

3. Report and Recommendation Construction: "a discrete component that collects data from one or more network components to which it is attached, filters or otherwise analyzes the data that has been collected, transmits noteworthy information, and receives feedback in order to update its capabilities of analysis"

4. The Court's Construction: "a component that collects data from one or more network components to which it is attached, filters or otherwise analyzes the data that has been collected, transmits noteworthy information, and receives feedback in order to update its capabilities of analysis."

BT faults the Report and Recommendation for using "discrete component" instead of "system" in the recommended construction. D.I. 141 at 19. The Magistrate Judge based this construction on her finding that "a 'probe' is a discrete component of a system, not itself a system." D.I. 141 at 21.

I agree that a probe can be a system and therefore will not adopt the recommended construction. The patents' written description uses the terms "probe/sentry system" and "probe" to refer to the same portion of the invention. In figure 1, component 2000 is labeled as a "Probe/Sentry" and further characterized as a "data collection and filtering system." Figure 2 shows the subcomponents of component 2000. Figure 2 is described in the written description as showing "an exemplary embodiment of a probe/sentry system." #237 patent at 8:35–36.

Elsewhere, the patents describe component 2000 as a "probe/sentry system." #237 at 5:37. Additionally, the patents' abstract refers to the "probe and other systems." #237 patent abstract.

The patents, however, do not define the term "system" and the parties have not proposed constructions of that term. In the absence of a clear construction as to what a "system" is, I believe construing "probe" to be a system would be at best unhelpful and at worst artificially narrow.

I also find no support in the patents for defining a probe as being a "discrete component." The patents use the word "discrete" only to describe incident tickets, #237 patent at 3:38–43, and nothing in the patents suggests that "a probe" must have a discrete housing or that it cannot be distributed across multiple subcomponents. The fact that the patents refer to "a probe" in the singular does not imply that the probe is contained entirely within a single housing. Rather, it merely indicates that "a probe" is an identifiable element. The patents also indicate that the probe can be implemented "in software or hardware or a combination of software and hardware." #237 patent at 4:48–50. It is not self-evident what requiring a software element to be "discrete" means. Thus, I do not believe it is appropriate to limit the disputed term to a "discrete component."

Instead of "system" or "discrete component," I believe the best word to use in the construction is "component," which covers both proposals. The patents

indicate that a system can be a component. #237 at 2:34–35, 3:4 (listing a "probe/sentry system" as a "component" in an exemplary implementation). Therefore, construing "a probe" as a "component" would allow, but not require, a probe to be a system.

For these reasons, I decline to follow the Report and Recommendation and will sustain BT's objection. I will construe "a probe" as "a component that collects data from one or more network components to which it is attached, filters or otherwise analyzes the data that has been collected, transmits noteworthy information, and receives feedback in order to update its capabilities of analysis."

IV. DISPUTED TERM FROM THE #641 PATENT

A. "information received about an identified potentially security-related event occurring on the network wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue" (#641 patent claim 18)

1. BT's Construction: The words of the claim term, as written, without the additional language

2. Fortinet's Construction: "information received from a probe about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified at the probe by filtering status data followed by an analysis of post-filtering residue"

3. Report and Recommendation's Construction: "information received from a probe about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified at the probe by filtering status data followed by an analysis of poster-filtering residue"

4. The Court's Construction: "information received from a probe about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified at the probe by filtering status data followed by an analysis of poster-filtering residue"

BT objects to the inclusion of "from a probe" and "at the probe" in the recommended construction. The Magistrate Judge found that BT's representations in the #641 patent's IPR proceeding were binding disclaimers. BT told the PTAB that claim 18 of the #641 patent "expressly contemplates transmission of information about identified events **from the probe** to the [secure operations center (SOC)] for a second level of analysis" and that the #641 patent claims in general "require an analysis of residue at the probe at the post-filtering stage, prior to transmission of information to the SOC." D.I. 89-5, Ex. Q at JA-0001534, JA-0001559 (emphasis in original). These statements were clear and unmistakable disclaimers. The Magistrate Judge found these and other similar representations to the PTAB "determinative" and I agree. D.I. 141 at 26.

BT argues that the recommended construction improperly adds a new apparatus (i.e., a probe) into a method claim about "an entirely different apparatus (i.e., the SOC)." D.I. 142 at 3. But construing claim 18 to clarify the relationship between an SOC and a probe does not change the claim from being directed to a method of operating an SOC. The recommended claim construction simply recognizes, as BT itself explains, that "[t]he claim . . . specifies the process by

which the information was generated *at the probe*." D.I. 142 at 4 (emphasis added).

Accordingly, I adopt the Magistrate Judge's recommendation and construe "information received about an identified potentially security-related event occurring on the network wherein the potentially security-related event is identified by filtering followed by an analysis of post-filtering residue" as "information received from a probe about an identified potentially security-related event occurring on the network, wherein the potentially security-related event is identified at the probe by filtering status data followed by an analysis of poster-filtering residue."

V. DISPUTED TERMS FROM THE #845 PATENT

A. "**suspect data**" (#845 patent, claims 1, 3, 9, 19, 20, 21, 23)

1. BT's Construction: "data indicating a possible security threat"
2. Fortinet's Construction: "data identified by one or more user computers, such computer(s) having concluded without aid from centralized analysis that the data indicates a possible security threat"
3. Report and Recommendation's Construction: "data identified by one or more user computers, such computer(s) having concluded without aid from centralized analysis that the data indicates a possible security threat"
4. The Court's Construction: "data identified as a possible security threat by one or more user computers without a centralized authority conducting any analysis to make that identification"

BT faults the recommended construction because it excludes decision-making involving aid from centralized analysis. D.I. 142 at 5. The parties agree "suspect data" is identified by one or more computers and indicates "a possible security threat." D.I. 141 at 35. The parties also do not dispute that the claimed invention is a system where user computers, rather than a central computer, are responsible for identifying malicious data and potential security threats. *See* D.I. 142 at 5; D.I. 146 at 4-5. The parties dispute, however, whether this arrangement allows for "aid from a centralized analysis."

Fortinet argues that BT disclaimed the aid of a central authority in identifying suspect data during the IPR proceedings and during prosecution. During the IPR, BT stated:

> The #845 Patent has two different embodiments for accomplishing [decentralized detection and action], one in which user computers detect suspect data and send a warning message to a group server for broadcast to all users within the group, and one in which each peer can detect suspect data and broadcast the detection of suspect data to all other peers. In both instances user computers identify "suspect" data and generate a unique signature, such as a hash, to identify it.
> . . .
> [T]he time from discovering a new virus to delivering its signature to protected machines took too long because an administrative authority was required to recognize the problem, identify the virus's signature, update the anti-virus database, and distribute the updated database. By the time this happened, it was often already too late.

D.I. 91-1, Ex. BB at JA-0002288, Ex. BB at JA-0002300 (internal citation omitted). And during prosecution the applicant stated that

> one characteristic of Applicant's claimed invention relates to the fact that it does not require a centralized analysis step. This arrangement advantageously speeds up the broadcast of warning messages between distributed user computers, one or more of which has itself identified the suspect data.
> . . .
> [I]t is precisely to avoid the requirement for such centralized detection of problems that Applicant has proposed and claimed a system where the user computers (of a given group) detect suspicious data and then exchange warning messages with each other on a distributed basis.

D.I. 88-4, Ex. H at JA-0000459–60 (emphasis in original).

Considering these statements in context, I believe the more natural reading of BT's statements is that the analysis to identify suspicious data happens independently at the user computer without assistance from a central authority. But BT's statements, which Fortinet and the Report and Recommendation rely on, do not unmistakably preclude the user computers from receiving information from a central authority beforehand. A self-contained analysis must take place at the user computer, but this analysis can make use of information (for example information about potential threats or known threat signatures) previously provided by a central authority so long as the user computer does not need to communicate with the central authority when actually conducting the analysis itself.

Accordingly, I agree with BT's objection and find the recommended construction unduly narrow.

But I also find that "aid from a centralized analysis" does not accurately capture the relationship between the user computer and the central authority. "Aid" implies that the central authority assists with the actual analysis. If the user computer relies on aid from the central authority in conducting the analysis, then detecting suspicious data would require centralized analysis—which is inconsistent with the claimed invention.

Accordingly, to credit BT's objections without omitting the important role of the user computers in the invention, I will construe "suspect data" to mean "data identified as a possible security threat by one or more user computers without a centralized authority conducting any analysis to make that identification."

B. "act in respect of any particular piece or set of suspect data when the count maintained therefor is substantially equal to or greater than at least one threshold value" (#845 patent claims 1, 19)

1. BT's Construction: The words of the claim term, as written, without the additional word "only"
2. Fortinet's Construction: "act in respect of any particular piece or set of suspect data only when the count maintained therefor is substantially equal to or greater than at least one threshold value"
3. Report and Recommendation's Construction: "act in respect of any particular piece or set of suspect data only when the count maintained therefor is substantially equal to or greater than at least one threshold value"

4. The Court's Construction: "act in respect of any particular piece or set of suspect data only when the count maintained therefor is substantially equal to or greater than at least one threshold value"

BT objects to the inclusion of "only" in the Magistrate Judge's recommended claim construction. D.I. 142 at D.I. 7. Fortinet responds that BT disclaimed the full scope of the term during prosecution as explained in the Report and Recommendation. D.I. 146 at 7.

To distinguish the #845 patent's claims 1 and 9 from the prior art, BT told the examiner that

> [i]nstead of acting . . . immediately upon detection of a potential threat, *no* action is taken in the invention of claims 1 and 19 until a pre-specified number of sightings of the data item is recorded. Specifically, a count is taken of the number of times the data item is through to be malicious, and action is taken only when the number exceeds a threshold value.

D.I. 88-4, Ex. H at JA-0000394 (emphasis in original). BT argues that this statement refers only to the claimed action, and that it does not mean other actions cannot happen. But this is not what the prosecution history statement says: it clearly states "no action" is taken until the threshold is reached. And BT has not identified any particular action that would not be covered by the quoted statement. This is a clear and unmistakable disclaimer.

BT argues that the disputed term appears in "comprising" claims, and therefore allows for unrecited actions. D.I. 142 at 7. But "comprising" language

does not allow a patentee to bypass a disclaimer during prosecution. *Bd. of Regents of the Univ. of Texas Sys. v. BENQ Am. Corp.*, 533 F.3d 1362, 1373 (Fed. Cir. 2008) (holding that plaintiff could not "rely on the word 'comprising' to broaden the scope of a claim phrase that was limited during prosecution so as to gain allowance of the patent."); *see also Spectrum Int'l, Inc. v. Sterilite Corp.*, 164 F.3d 1372, 1380 (Fed. Cir. 1998) ("'Comprising' is not a weasel word with which to abrogate claim limitations").

Accordingly, I will adopt the Magistrate Judge's recommendation and construe "act in respect of any particular piece or set of suspect data when the count maintained therefor is substantially equal to or greater than at least one threshold value" as "act in respect of any particular piece or set of suspect data only when the count maintained therefor is substantially equal to or greater than at least one threshold value."

VI. DISPUTED TERM FROM THE #358 PATENT

A. "a message-exchange system including the exchange of group specific tags" (#358 patent claim 26, 50)

1. BT's Construction: "a system that facilitates agent communications, including the communication of group specific tags"
2. Fortinet's Construction: "a system for hindering the spread of attacks to agents in other groups using group-specific tags"
3. Report and Recommendation's Construction: "a system for hindering the spread of attacks to agents in other groups using group-specific tags"

4. The Court's Construction: "a system for hindering the spread of attacks to agents in other groups using group-specific tags"

BT argues that the Report and Recommendation's construction of the disputed term "is premised on a flawed reading of the prosecution history." D.I. 142 at 8. I disagree, and for the reasons articulated by the Magistrate Judge, I will adopt her construction of the term.

* * * *

Now therefore, at Wilmington on this Fifth day of August in 2021, it is HEREBY ORDERED that:

1. Plaintiffs' Objections to the April 15, 2021 Report and Recommendations Concerning Claim Construction (D.I. 142) are OVERRULED-IN-PART and SUSTAINED-IN-PART;

2. Defendant Fortinet, Inc.'s Objections to April 15, 2021 Report and Recommendation Regarding Claim Construction (D.I. 143) are OVERRULED;

3. The April 15, 2021 Report and Recommendation (D.I. 141) is ADOPTED-IN-PART and REJECTED-IN-PART; and

4. The parties shall submit for the Court's signature no later than August 23, 2021 a claim construction order consistent with this Memorandum Order, the Magistrate Judge's claim constructions that were not objected to, and the claim constructions previously agreed to by the parties.

CHIEF JUDGE